



## BIDDER INQUIRY RESPONSES

### To a Request for Proposal (RFP) for an Audit of Information Technology & Systems at the Colorado Department of Public Health and Environment (CDPHE)

October 13, 2016

1. Why is this audit being commissioned?

**Response:** *The audit is being commissioned based on risk and the State Auditor's discretion.*

2. Has this or an audit with a similar scope of work been performed previously? If so, who performed it, what was the cost, and how many hours were expended on the project?

**Response:** *This or another audit with similar scope has not been performed previously.*

3. Does the OSA anticipate physical site visits will be required to the 5 remote sites listed in the RFP?

**Response:** *Although physical site visits to the remote sites listed in the RFP may be necessary to fully achieve the audit objectives, it is anticipated that most of the audit work will involve the Governor's Office of Information Technology (OIT) and the Office of Information Security (OIS), which have primary physical locations in the Denver metro area. In addition, it is anticipated that most of the audit work involving CDPHE business management and staff could be performed out of its primary Denver metro locations, without the need for additional remote site visits.*

4. Would the OSA consider disclosing the three systems to be included within the scope of this audit? We may have specific prior experience with these systems that could be beneficial in performance of the audit.

**Response:** *Not at this time; the three preselected systems will be disclosed to the selected contractor upon contract award.*

5. Will direct communication with management of the systems within audit scope be available during testing or will the contracted auditor be expected to flow all communication through the liaison?



We Set the Standard for Good Government

**Response:** *Direct communications with the management of the systems within the scope of the audit should be made available during the audit and testing. The audit may also have one or more audit liaisons to assist with communication flows. Any such communication expectations should be established as needed during project initiation and planning communications with the auditee.*

6. Reference Section 1, B (pages 3-4) and Section 1, C, item 3.b.iii (page 10). How many of the Department's 6 locations are in scope for the audit? For example, would the physical security of all 6 locations need to be assessed for the audit, or could a sample of locations be assessed? Are there any specific Department locations that must be assessed for physical security (e.g.: locations with Departmental data center(s) where the in-scope systems are hosted); and, if so, which locations?

**Response:** *Refer to #3 above. In addition, there are no predetermined requirements to test physical security at all sites as a part of this audit, and appropriate sampling methodologies can be applied, if needed, to complete the audit objectives. That said, the data centers for the in-scope systems are all said to be located in the Denver metro area. In addition, although the OSA has done preliminary information gathering related to the preselected systems, additional detail related to this area (i.e., physical security) and all other areas noted in the RFP should be obtained by the selected contractor during the audit planning phase and when working with the auditee to gain a better understanding of the system environments and the specific details that are necessary to complete the audit objectives.*

7. Reference Section 1, B (page 4). We understand that the 3 Departmental systems in scope will be disclosed to the selected vendor, but is there any general information related to these systems that can be shared during the proposal process such as:
- a. Are any of the systems externally facing (i.e.: accessible from the Internet); and, if so, how many?
  - b. Are all of the systems using a "client server" type of architecture?
  - c. Are any of the systems mainframe based; and, if so, how many?
  - d. What operating systems are used to host the in-scope systems (i.e.: are they Windows-based, Unix-based, etc.)?
  - e. Are any of the systems in-scope hosted outside of the Department's facilities? If so, how many and where are they hosted?

**Response:** *Preliminary general information about the preselected in-scope systems has been obtained by the OSA. This information will be disclosed to the selected contractor upon contract award. However, to address these specific questions, we can indicate the following at this time, based on the preliminary information we have obtained:*

- a. *It appears that two of the three systems are remotely accessible, with at least one having a web interface.*
- b. *It appears that all of the systems have client/server architectures.*
- c. *It appears that none of the systems are mainframe-based.*

- d. It appears that all of the systems are Windows-based.*
- e. It appears that none of the in-scope systems are hosted outside of the State's facilities. However, if any are found to be outsourced or hosted by service providers after further information is gathered by the selected contractor, they should not be included in the audit scope, as noted in the RFP on pg. 9.*

*Any additional information needed to complete the audit objectives should be obtained by the selected contractor when working with the auditee to gain a better understanding of the system environments during the audit planning phase.*

8. Reference Section 1, C (page 7), second bullet on the page. How many additional findings meetings should we anticipate with CDPHE oversight bodies? If the number of meetings is unknown, can we include an assumption in our pricing for a maximum or specified number of meetings?

***Response:*** *It is rare that the OSA holds additional findings meetings to brief audited agencies' oversight bodies. However, there are three oversight bodies that could potentially be involved as noted below:*

- *House Public Health Care and Human Services Committee -- This committee has legislative oversight responsibility for the Department of Public Health and Environment and considers matters regarding state health care programs and social services*
- *Senate Health and Human Services Committee--This committee has legislative oversight responsibility for the Department of Public Health and Environment and considers matters regarding state health and welfare programs, health insurance, social services, and environmental health.*
- *Joint Technology Committee-- This joint House and Senate committee has legislative oversight responsibility for the Governor's Office of Information Technology and considers matters regarding state information technology.*

*Given this information, the number of meetings is unknown, and an assumption in your pricing for a maximum or specified number of meetings can be included in your pricing.*

9. Reference Section 1, C (page 8). If additional systems (beyond the 3 pre-selected by the OSA), are identified for inclusion in the scope of the audit and agreed to by the OSA, will the additional level of effort and costs required to include these systems be negotiated for contract amendment?

***Response:*** *The OSA is asking for an up-front proposal that includes all costs and level of effort given the objectives and scope outlined in the RFP. If, however, additional systems (beyond the 3 pre-selected by the OSA) are identified for inclusion in the scope of the audit and agreed to by the OSA, additional level of effort and costs required to include these systems would be negotiated, and any subsequent corresponding contract amendments would ensue, if necessary.*

10. Reference Section 1, C (page 9), second paragraph; and Section 1, C, item 2.i (page 10). Our understanding of this paragraph is that all of the selected, in-scope Departmental systems are maintained by either the Department or OIT and that all in-scope services and processes are performed by either the Department or OIT; therefore, the audit requested would not require interaction with any third-party service providers to either the Department or OIT. Is that correct?

**Response:** *This understanding would be correct, based on the preliminary information the OSA has obtained on the preselected systems. If any of the in-scope systems are found to be outsourced or hosted by service providers after further information is gathered by the selected contractor, they should not be included in the audit scope, as noted in the RFP on pg. 9.*

11. Reference Section 1, C, item 4 (page 11). Would completion of work related to Information Systems Acquisition, Development, and Implementation require requesting information from or interacting with entities or personnel outside of the Department (i.e.: have any of the system development and implementation efforts been performed by external third-party providers or contractors)? Additionally, is there a maximum sample size of projects that should be considered for testing or can we include an assumption in our pricing for a maximum or specified number of projects

**Response:** *The intent of this work is to review the internal, state-managed processes and controls related to Information Systems Acquisition, Development, and Implementation (i.e., those processes and controls managed and operated by the Department and OIT). Based on the preliminary information the OSA has obtained on the preselected systems, it appears that all three are state-managed systems and two of the three are currently or will soon be undergoing development and/or implementation in the relative near future. Additional detail related to this area, and all other areas noted in the RFP, should be obtained by the selected contractor during the audit planning phase and when working with the auditee to gain a better understanding of the system environments and the specific details that are necessary to complete the audit objectives. Then, an appropriate sampling methodology can be determined and applied by the selected contractor, if necessary, based on additional risk assessment procedures performed during the audit planning phase. If any of the in-scope systems are found to be outsourced or hosted by service providers after further information is gathered by the selected contractor, they should not be included in the audit scope, as noted in the RFP on pg. 9.*

12. For the 3 Departmental systems in scope is there an audit period in mind or can we include an assumption of the previous 12 months for the audit period?

**Response:** *The OSA is interested in the design and operating effectiveness of the current IT and information security control environment related to the process areas noted in the RFP. As such, the selected contractor should perform risk assessment*

*procedures during the planning phase, and work with the OSA, as needed, to determine an appropriate time period for the areas noted in the RFP that are to be reviewed during the audit. For example, although, the previous 12 months may be an appropriate audit period to review most of the process and control areas noted in the RFP, if any of these areas would require different time frames to adequately review them and achieve the audit objectives, the audit period should be determined and applied more selectively for each of these areas, as necessary. For example, the previous 12 months may not be an appropriate timeframe to adequately review the processes and controls within the Information Systems Acquisition, Development, and Implementation area, and a more appropriate time frame should be determined and applied by the selected contractor in order to achieve the audit objectives.*

13. For the three systems to be examined, can OSA provide the OS and database versions used?

**Response:** *Not at this time. The preliminary general information obtained by the OSA on the three preselected in-scope systems will be disclosed to the selected contractor upon contract award. Any additional information needed to complete the audit objectives should be obtained by the selected contractor when working with the auditee to gain a better understanding of the system environments during the audit planning phase.*

14. How many users per system?

**Response:** *This information is not available at this time and should be obtained by the selected contractor during the audit planning phase.*

15. Are there regulatory requirements, such as HIPAA, that should be included in the audit testing?

**Response:** *As CDPHE is responsible for improving and protecting the health of people in Colorado, it is reasonable to expect that HIPAA requirements would impact audit testing. Any additional information needed to address this question and complete the audit objectives should be obtained by the selected contractor when working with the auditee to gain a better understanding of the system environments during the audit planning phase.*

16. Has the OSA conducted an audit of this environment before? If so, can the OSA make the SOC 1 report and other applicable reports available to review?

**Response:** *Refer to #2 above.*

17. Would the OSA be amenable to extending the deadline by one week to allow proposers the opportunity to incorporate QA into our responses?

**Response:** *Due to the timeframe of the audit deadlines, we are unable to extend the due date for proposals.*

18. Could the OSA please provide a copy of Exhibit G for review?

**Response:** *Exhibit G was included within Section IV of the RFP, starting on page 19.*

19. Would the OSA prefer that the audit is conducted as a Performance Audit, AT-601, or AT 101 examination standards?

**Response:** *As stated in the RFP, on page 5, the OSA prefers the audit to be conducted in accordance with generally accepted government auditing standards (Yellow Book) for performance audits.*

20. What are circumstances driving this audit?

**Response:** *Refer to #1 above.*

21. Can the State provide the relevant size of each system to be tested e.g., number of servers, workstations, etc.?

**Response:** *This information is not available at this time and should be obtained by the selected contractor during the audit planning phase.*

22. How many sites are within the scope of the engagement? What are their relative distances from where the main audit function is to be performed?

**Response:** *Refer to #6 above.*

23. Will related diagrams, policies, and procedures required to perform the assessments be provided to the Contractors prior to each system assessment for analysis? Can the Contractors retain that information offsite in its own protected network for analysis?

**Response:** *The selected contractor should work with the management and staff at CDPHE and OIT to obtain any diagrams, policies, procedures, or other information needed to adequately achieve the audit objectives. As noted in the OSA's standard contract template, which is included in "Section IV – Supplemental Information" of the RFP, the audit work papers shall be the exclusive property of the contractor, and therefore, the selected contractor shall retain all audit work papers and information obtained as a part of this audit, whether in its own protected network or otherwise. Given this, the selected audit contractor will be required to protect the audit work papers and other information obtained as a part of this audit by implementing appropriate security controls in accordance with, at a minimum, the information security policy requirements, as stated in "Exhibit E – Information Security Policy For Contractors."*

24. Does the State have a preferred framework for the assessments, e.g. NIST?

**Response:** *Please refer to page 11 of the RFP.*

25. Does the State prefer a single deliverable for each assessment performed or will all three assessments be aggregated into one report?

**Response:** *The audit and any findings and conclusions will be included within one report, although it is possible that the audit report will be composed of two separate reports, one public report and one confidential report, as noted in the RFP on page 7.*

26. Does the State expect an external (web facing) and internal vulnerability scans of the host environments to be assessed? If so, will this be “white box” testing?

**Response:** *The selected contractor is not expected to perform a vulnerability assessment or penetration test as a part of this audit. Please see the audit purpose, objectives, and scope as outlined in the RFP, starting on page 8.*

27. Will Contractors be given privileged rights to perform vulnerability scanning if scanning is desired?

**Response:** *N/A – refer #26 above.*

28. Have the IT controls been explicitly documented by the process owners in the IT environment?

**Response:** *This information is not available at this time and should be obtained by the selected contractor during the audit.*

29. Please provide the audit period for the OE testing (example: 10/1/xx – 9/30/xx).

**Response:** *Refer to #12 above.*

30. Have the IT controls been designed and implemented for the entire audit period identified in question #29?

**Response:** *This information is not available at this time and should be obtained by the selected contractor during the audit.*

31. Does the IT personnel as well as the three subject IT systems reside in predominately one location? Please disclose the locations for the IT systems where we should plan to perform the testing

**Response:** *Refer #6 above.*

32. Does management plan to make an assertion related to the design and operating effectiveness of the IT environment for purposes of an attest engagement?

**Response:** *No, a management assertion is not expected as a part of this audit. As stated in the RFP on page 5, the OSA prefers this audit to be conducted in accordance with generally accepted government auditing standards (Yellow Book) for performance audits.*

33. Will the cost of the 100 hard copies of the bound printed final report be a reimbursable cost to the contractor?

**Response:** *The 100 hard copies are not a firm number, as indicated on page 8 of the RFP. However, the printing and binding costs of 100 hard copies, or an agreed-upon number of hard copies, should be included within the proposal amount.*

34. Are the “three significant departmental systems that have been included in the scope of this audit” (page 8) commercial off the shelf (COTS) products or systems that were custom developed by, or on behalf of, the State of Colorado?

**Response:** *Based on the preliminary information the OSA has obtained, it appears that two of the three systems were internally developed and customized for their specific needs. The third system appears to have been externally developed, but the OSA has not determined the level of customization of this system. Additional detail should be obtained by the selected contractor during the audit planning phase and when working with the auditee to gain a better understanding of the system environments and the specific details necessary to complete the audit objectives.*

35. For the three preselected systems, are all interfaces between those systems and other systems considered in scope for the audit? If so, please identify the number of interfaces that exist for each system?

**Response:** *The number of system interfaces is not available at this time, and the selected contractor should perform risk assessment procedures during the audit planning phase and work with the OSA, as needed, to determine which, if any, interfaces should be included in the scope of this audit to achieve the audit objectives. If needed, appropriate sampling methodologies can be applied to test any interface controls determined to be in-scope.*

36. Regarding SOW Item #1 – IT and Information Security Governance and Management (page 9) – are there different governance structures and information security policies and strategies for each of the 3 preselected departmental systems?

**Response:** *Based on the preliminary information obtained by the OSA, the governance structures and information security policies and strategies are expected to be consistent across the three preselected departmental systems. However, any additional*

*information needed to verify this and complete the audit objectives should be obtained by the selected contractor when working with the auditee to gain a better understanding of this area during the audit.*

37. For scope of work item #4 Information Systems Acquisition, Development and Implementation (page 11) – is it the Office of the State Auditor’s (OSA’s) expectation that the sample for this component of the work is different from the 3 preselected systems for SOW Items 1-3?

***Response:*** *It is possible the sample may be different from the three preselected systems. However, refer to #38 below.*

38. For scope of work item #4 Information Systems Acquisition, Development and Implementation (page 11) – how many such “acquisitions, developments, or implementation projects” has CDPHE undertaken during the past 3 calendar years?

***Response:*** *This information is not available at this time and should be obtained by the selected contractor during the audit planning phase.*

39. For scope of work item #4 Information Systems Acquisition, Development and Implementation (page 11) – how many “acquisitions, developments, or implementation projects” does the OSA consider to be an adequate sample?

***Response:*** *Adequate sample sizes should be determined by the selected contractor based on the information gathered and the risk assessment procedures performed during the planning phase of the audit.*

40. For scope of work item #4 Information Systems Acquisition, Development and Implementation (page 11) – does OSA expect that this work will be performed only on those projects that have been completed, or will this potentially cover initiatives that are in-progress.

***Response:*** *To adequately review the areas noted in this section, the scope may need to include completed and in-progress system acquisitions, developments, or implementations. As such, an appropriate system sample should be determined by the selected contractor based on the information gathered and the risk assessment procedures performed during the audit planning phase.*

41. What is the Office of the State Auditor’s budget for this Audit?

***Response:*** *This information is not available to potential bidders. The selected contractor should propose a budget to ensure that the audit work is completed by the established time frames, as stated within the RFP.*

42. Is there a previous audit report? If so can we review it?

**Response:** *No, refer to #2 above.*

43. If there was a prior audit(s), will the selected vendor have access to the prior audit work papers?

**Response:** *N/A - refer to #42 above.*

44. Does CDPHE have an existing audit program and risk/controls matrix or will one need to be created?

**Response:** *An audit program and risk/controls matrix will need to be developed by the selected contractor after performing appropriate audit planning and risk assessment procedures.*

45. How many active users does each application have?

**Response:** *Refer to #14 above.*

46. How many buildings/locations are in-scope? How many data centers?

**Response:** *Refer to # 6 above.*

47. Does CDPHE manage its own IT infrastructure?

**Response:** *The Office of Information Technology provides IT infrastructure support to CDPHE.*

48. If additional systems are brought into scope (beyond the initial three), will the selected vendor have an opportunity to reassess the number of hours/fees included in the project?

**Response:** *Refer to #9 above.*

49. Does CDPHE have a complete set of IT policies and procedures?

**Response:** *This information is not available at this time and should be obtained by the selected contractor during the audit.*

50. Does CDPHE utilize any cloud-based services? Would any of these be considered in-scope?

**Response:** *This information is not available at this time and the selected contractor should perform risk assessment procedures during the audit planning phase and work with the OSA, as needed, to determine which, if any, cloud-based services should be included in the scope of this audit to achieve the audit objectives. If needed, appropriate sampling methodologies can be applied to test any such services determined to be in-scope.*